1/5/1 (Item 1 from file: 351)
DIALOG(R)File 351:Derwent WPI

013461376 **Image available**
WPI Acc No: 2000-633319/ **200061**
XRPX Acc No: N00-469338

Security system has IC card reader-writer to rewrite valid access information in access key of user to invalid access information when operating system is not operated within preset time after permitting access

Patent Assignee: HITACHI COMPUTER ELECTRONICS KK (HITA-N)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2000259277	A	20000922	JP 9964966	A	19990311	200061	B

Priority Applications (No Type Date): JP 9964966 A 19990311
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2000259277	A		9	G06F-001/00	

Abstract (Basic): **JP 2000259277** A

NOVELTY - Each authenticated user has access key to store user validity details for accessing operating system (206) of computer (103). User's access key is read and validated by IC card reader-writer to permit access to operating system. When user does not operate operating system within preset time, his access right is prohibited and IC card reader-writer rewrites information in access key to be invalid.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for security procedure.

USE - In computer system for authentication of user.

ADVANTAGE - Since the IC card reader-writer rewrites validity to access information stored in access key as invalidity to access, access of system by third person is eliminated.

DESCRIPTION OF DRAWING(S) - The figure shows the software configuration of electronic computer system.

Computer (103)
Operating system (206)
pp; 9 DwgNo 2/5

Title Terms: SECURE; SYSTEM; IC; CARD; READ; WRITING; REWRITING; VALID; ACCESS; INFORMATION; ACCESS; KEY; USER; INVALID; ACCESS; INFORMATION; OPERATE; SYSTEM; OPERATE; PRESET; TIME; AFTER; PERMIT; ACCESS
Derwent Class: T01
International Patent Class (Main): G06F-001/00
International Patent Class (Additional): G06F-015/00
File Segment: EPI

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－259277
（P2000－259277A）
(43)公開日　平成12年９月22日(2000.9.22)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　1/00	３７０	Ｇ０６Ｆ　1/00	３７０Ｅ	５Ｂ０８５
15/00	３３０	15/00	３３０Ｇ	

審査請求　未請求　請求項の数６　ＯＬ　（全９頁）

(21)出願番号　特願平11－64966

(22)出願日　平成11年３月11日(1999.3.11)

(71)出願人　000153454
株式会社日立インフォメーションテクノロジー
神奈川県足柄上郡中井町境456番地
(72)発明者　中道　聡
神奈川県秦野市堀山下１番地　株式会社日立インフォメーションテクノロジー内
(72)発明者　春山　和博
神奈川県秦野市堀山下１番地　株式会社日立インフォメーションテクノロジー内
(74)代理人　100087170
弁理士　富田　和子

Ｆターム(参考)　5B085 AE12 AE13

(54)【発明の名称】　セキュリティシステムおよびセキュリティ方法

(57)【要約】
【課題】アクセスキーをシステムに接続したまま放置された場合に、第三者によるシステムへの不正なアクセスを排除する。
【解決手段】電子計算機１０３のアクセスキー処理プログラム２０５は、使用可能／不可判別用データ２０２に使用可能を表すデータが書き込まれた正当なアクセスキー１０１がＩＣカードリーダライタ１０２に接続されると、ＯＳ２０６を動作させ、利用者にシステムへのアクセスを認めるが、その後、一定時間以上、利用者よりの入力が無かった場合には、アクセスキー１０１が放置されたものと見なして、ＯＳ２０６を停止させ、かつ、アクセスキー１０１の使用可能／不可判別用データ２０２を使用不可を表すデータに書き換えＯＳ２０６を動作させることができないようにすることにより、他者のシステムへの不正なアクセスを排除する。

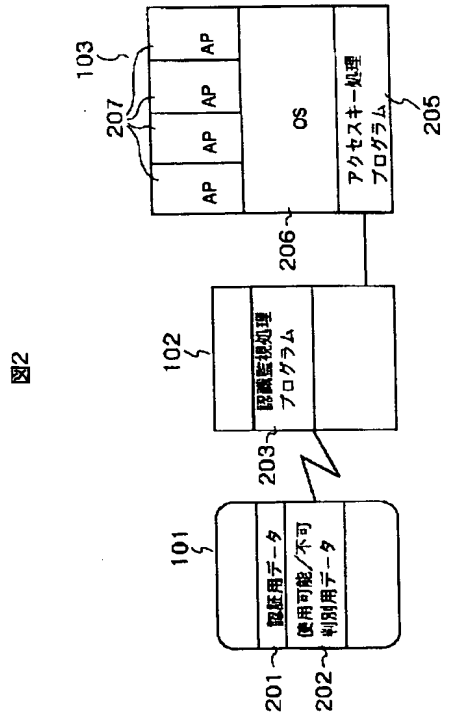


図2

1

【特許請求の範囲】

【請求項１】保護対象システムへのアクセスを許可する利用者を限定するセキュリティシステムであって、

利用者を認証するための認証用データと、アクセスキーの有効／無効を表す使用可否データとを記憶したアクセスキーに対して読み書きを行うアクセスキー読み書き手段と、

前記アクセスキー読み書き手段を介して前記アクセスキーから読み出した認証用データから前記保護対象システムへのアクセスを許可する利用者を認証でき、かつ、前記アクセスキー読み書き手段を介して前記アクセスキーから読み出した前記使用可否データが当該アクセスキーが有効である旨を示す場合に、利用者の前記保護対象システムへのアクセスを許可するアクセス許可手段と、

利用者の前記保護対象システムへのアクセスを許可した後、所定期間以上、利用者が前記保護対象システムへの入力を行わなかった場合に、利用者の前記保護対象システムへのアクセスを禁止すると共に、前記アクセスキーの使用可否データを、当該アクセスキーが無効である旨を示す使用可否データに書き換えるアクセスキー無効化手段とを有することを特徴とするセキュリティシステム。

【請求項２】請求項１記載のセキュリティシステムであって、

前記アクセスキー読み書き手段を介して前記アクセスキーから読み出した認証用データから前記保護対象システムへのアクセスを許可する利用者を認証でき、かつ、前記アクセスキー読み書き手段を介して前記アクセスキーから読み出した前記使用可否データが当該アクセスキーが無効である旨を示す場合に、利用者より、利用者を認証可能な情報の入力を受け付け、受け付けた情報から、前記保護対象システムへのアクセスを許可する利用者を認証できた場合に、利用者の前記保護対象システムへのアクセスを許可すると共に、前記アクセスキーの使用可否データを、当該アクセスキーが有効である旨を示す使用可否データに書き換えるアクセスキー有効化手段を有することを特徴とするセキュリティシステム。

【請求項３】保護対象システムへのアクセスを許可する利用者を限定するセキュリティ方法であって、

利用者を認証するための認証用データと、アクセスキーの有効／無効を表す使用可否データとを記憶したアクセスキーから読み出した認証用データから前記保護対象システムへのアクセスを許可する利用者を認証でき、かつ、前記アクセスキーから読み出した前記使用可否データが当該アクセスキーが有効である旨を示す場合に、利用者の前記保護対象システムへのアクセスを許可し、

利用者の前記保護対象システムへのアクセスを許可した後、所定期間以上、利用者が前記保護対象システムへの入力を行わなかった場合に、利用者の前記保護対象システムへのアクセスを禁止すると共に、前記アクセスキーの使用可否データを、当該アクセスキーが無効である旨を示す使用可否データに書き換えることを特徴とするセキュリティ方法。

2

【請求項４】電子計算機に読み取られ実行されるプログラムを記憶した記憶媒体であって、

前記プログラムは、前記電子計算機に、

利用者を認証するための認証用データと、アクセスキーの有効／無効を表す使用可否データとを記憶したアクセスキーから読み出した認証用データから前記保護対象システムへのアクセスを許可する利用者を認証でき、かつ、前記アクセスキーから読み出した前記使用可否データが当該アクセスキーが有効である旨を示す場合に、利用者の前記保護対象システムへのアクセスを許可するステップと、

利用者の前記保護対象システムへのアクセスを許可した後、所定期間以上、利用者が前記保護対象システムへの入力を行わなかった場合に、利用者の前記保護対象システムへのアクセスを禁止すると共に、前記アクセスキーの使用可否データを、当該アクセスキーが無効である旨を示す使用可否データに書き換えるステップとを実行させることを特徴とする記憶媒体。

【請求項５】保護対象システムへのアクセスを許可する利用者を限定するセキュリティシステムであって、

利用者を認証するための認証用データを記憶したアクセスキーに対して読み書きを行うアクセスキー読み書き手段と、

各アクセスキーの有効／無効を表す使用可否データを記憶する使用可否データ記憶手段と、

前記アクセスキー読み書き手段を介して前記アクセスキーから読み出した認証用データから前記保護対象システムへのアクセスを許可する利用者を認証でき、かつ、前記使用可否データ記憶手段に記憶された前記使用可否データが当該アクセスキーが有効である旨を示す場合に、利用者の前記保護対象システムへのアクセスを許可するアクセス許可手段と、

利用者の前記保護対象システムへのアクセスを許可した後、所定期間以上、利用者が前記保護対象システムへの入力を行わなかった場合に、利用者の前記保護対象システムへのアクセスを禁止すると共に、前記前記使用可否データ記憶手段に記憶された使用可否データを、当該アクセスキーが無効である旨を示す使用可否データに書き換えるアクセスキー無効化手段とを有することを特徴とするセキュリティシステム。

【請求項６】請求項１、２または５記載のセキュリティシステムと、前記保護対象システムとを有し、前記保護対象システムは、電子計算機上で稼働するシステムであることを特徴とする電子計算機システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、システムへのアク

セスを許可する利用者の認証にアクセスキーを用いる技術に関するものである。

【０００２】

【従来の技術】電子計算機上に構築されるシステムのセキュリティを高めるためにシステムへのアクセスを特定の利用者に限定する技術として、アクセスキーを利用者の認証に用いる次のような技術が知られている。

【０００３】すなわち、この技術では、あらかじめ、システム（ＯＳや特定のアプリケーション）へのアクセスを認める特定の利用者に、認証用の情報を記憶させたＩＣカードをアクセスキーとして配布する。そして、アクセスキーを配布された利用者は、システム利用開示に、このアクセスキーをシステムに電気的または電磁気的に接続し読み取らせる。システムは読み取ったアクセスキーに記憶された認証用の情報が正規のものであれば、利用者にシステムへのアクセスを許可する。

【０００４】そして、システムへのアクセスを許可した後も、引き続きアクセスキーを監視し、正規の認証用の情報が記憶されているアクセスキーを認識できなくなると、再度、正規の認証用の情報が記憶されているアクセスキーを認識できるまで、システムを停止する。

【０００５】このようなアクセスキーを利用者の認証に用いる技術によれば、利用者は、自分がシステムへアクセスする権限を有することをシステムに示すために、認証用の情報（たとえば個人ＩＤやパスワードなど）をキーボードなどから、システム利用の度にいちいち入力する必要がなくなる。また、システム利用途中で、システムを離れる場合も、アクセスキーを共に持ち去れば、この間に第三者が不正にシステムにアクセスすることを排除することができる。

【０００６】

【発明が解決しようとする課題】前記従来のアクセスキーを利用者の認証に用いる技術によれば、システム利用途中でアクセスキーをシステムに接続したまま、利用者がシステムを離れてしまった場合には、この間に第三者が、このアクセスキーを用いて不正にシステムにアクセスすることが可能となる。また、そのまま第三者にアクセスキーを持ち去られてしまった場合には、その後に、このアクセスキーを用いた第三者によってシステムに不正にアクセスされてしまう可能性がある。

【０００７】そこで、本発明は、システム利用途中でアクセスキーをシステムに接続したまま、利用者がシステムを離れてしまった場合に、第三者による、システムへの不正なアクセスを排除することを課題とする。

【０００８】

【課題を解決するための手段】前記課題達成のために、本発明は、たとえば、保護対象システムへのアクセスを許可する利用者を限定するセキュリティシステムであって、利用者を認証するための認証用データと、アクセスキーの有効／無効を表す使用可否データとを記憶したアクセスキーに対して読み書きを行うアクセスキー読み書き手段と、前記アクセスキー読み書き手段を介して前記アクセスキーから読み出した認証用データから前記保護対象システムへのアクセスを許可する利用者を認証でき、かつ、前記アクセスキー読み書き手段を介して前記アクセスキーから読み出した前記使用可否データが当該アクセスキーが有効である旨を示す場合に、利用者の前記保護対象システムへのアクセスを許可するアクセス許可手段と、利用者の前記保護対象システムへのアクセスを許可した後、所定期間以上、利用者が前記保護対象システムへの入力を行わなかった場合に、利用者の前記保護対象システムへのアクセスを禁止すると共に、前記アクセスキーの使用可否データを、当該アクセスキーが無効である旨を示す使用可否データに書き換えるアクセスキー無効化手段とを有することを特徴とするセキュリティシステムを提供する。

【０００９】このようなセキュリティシステムによれば、、正当なアクセスキーが提示されると、利用者に保護対象システムへのアクセスを許可するが、その後、一定時間以上、利用者よりの何の入力も無かった場合には、アクセスキーの正当な所持者がアクセスキーを放置したものと見なして、保護対象システムへのアクセスを禁止し、かつ、アクセスキーの使用可否データを無効を表すデータに書き換え、このアクセスキーによって保護対象システムへのアクセスが許可されないようにすることにより、他者の不正なアクセスを排除することができる。

【００１０】

【発明の実施の形態】以下、本発明の実施形態を説明する。

【００１１】図１に本実施形態に係る電子計算機システムの構成を示す。

【００１２】図示するように、本実施形態に係る電子計算機システムは、電子計算機（以下、「ＰＣ」と記す）１０３と、ＩＣカードを用いたアクセスキー１０１の読み書きを行うＩＣカードリーダライタ１０２より構成される。

【００１３】ＩＣカードリーダライタ１０２は、ＰＣ１０３と接続されており、ＰＣ１０３から制御することができる。

【００１４】次に、本電子計算機システムのソフトウエア構成を図２に示す。

【００１５】図示するように、ＰＣ１０３は、アクセスキー処理プログラム２０５、ＯＳ２０６、ＯＳ２０６上で稼働するアプリケーションプログラム２０７が組み込まれている。ただし、アクセスキー処理プログラム２０５はＯＳ２０６の一部として、ＯＳ２０６に組み込まれるものであってもよい。また、ＩＣカードリーダライタ１０２は、ＩＣカードリーダライタ１０２内部に備えられたプロセッサで実行される認識監視処理プログラム２

０３が組み込まれている。また、アクセスキー１０１には、認証用データ２０１と使用可能／不可判別用データ２０２が記憶される。

【００１６】なお、ＰＣ１０３のハードウエア構成は、図３に示すように、ＣＰＵ３０１、主記憶３０２、入力装置３０３、表示装置３０４、外部記憶装置３０５、３０６、外部入出力インタフェース３０８などを備えた一般的な電子計算機の構成を有する。

【００１７】このようなハードウエア構成において、アクセスキー処理プログラム２０５、ＯＳ２０６、アプリケーションプログラム２０７の各プログラムは、外部記憶装置３０５、３０６に記憶されており、ＣＰＵ３０１は、外部記憶装置３０５、３０６に記憶されたこれらプログラムを主記憶３０２にロードし実行する。なお、これらのアクセスキー処理プログラム２０５、ＯＳ２０６、アプリケーションプログラム２０７は、外部記憶装置３０６にマウントされたリムーバルな記憶媒体３０７から、直接、もしくは、一旦、他の外部記憶装置３０５に記憶された後、主記憶３０２にロードされるものであってよい。

【００１８】以下、このような電子計算機システムの動作について説明する。

【００１９】まず、ＩＣカードリーダライタ１０２の認識監視処理プログラム２０３の動作について説明する。

【００２０】図４に、認識監視処理プログラム２０３の動作の手順を示す。

【００２１】図示するように、ＩＣカードリーダライタ１０２が起動されると、認識監視処理プログラム２０３は起動され、ＰＣ１０３からの命令待ちの状態となる。そして、ＰＣ１０３からアクセスキー１０１の認識監視の開始命令を受け付けると（ステップ４０１）、まず、アクセスキー１０１の認証用データ２０１と使用可能／不可判別用データ２０２を電気的または電磁気的に読み出し（ステップ４０２）、これらを読み込めた場合には（ステップ４０３）、これまで同データを記憶したアクセスキー１０１を認識していたか否かを調べる（ステップ４０６）。ここでは、具体的には、前回行ったステップ４０２で認証用データ２０１と使用可能／不可判別用データ２０２が読み出されており、かつ、今回行ったステップ４０２で読み出した認証用データ２０１と使用可能／不可判別用データ２０２が前回行ったステップ４０２で読み出した認証用データ２０１と使用可能／不可判別用データ２０２と同じである場合には、これまで同データを記憶したアクセスキー１　０１を認識していたと判定し、他の場合には、これまで同データを記憶したアクセスキー１０１を認識していなかったと判定する。但し、今回行ったステップ４０２が起動後最初に行われたステップ４０２である場合には、これまで同データを記憶したアクセスキー１０１を認識していなかったと判定する。

【００２２】そして、ステップ４０６で、これまで同データを記憶したアクセスキー１０１を認識していたと判定された場合には、ステップ４１１に進む。

【００２３】一方、ステップ４０６で、読み出した使用可能／不可判別用データ２０２が使用可能を表しているかどうかを判定し（ステップ４０８）、使用可能を表していると判定された場合には、ＰＣ１０３へ使用可能のアクセスキー１０１を認識した事を今回行ったステップ４０２で読み出した認証用データ２０１と共に報告し（ステップ４１０）、使用不可を表していると判定された場合には、ＰＣ１０３へ使用不可のアクセスキー１０１を認識した事を今回行ったステップ４０２で読み出した認証用データ２０１と共に報告する（ステップ４０９）。そして、ステップ４１１に進む。

【００２４】この結果、ＩＣカードリーダライタ１０２に使用可能／不可判別用データ２０２が使用可能を表しているアクセスキー１０１が電気的又は電磁気的に接続されると、その時点（ＩＣカードリーダライタ１０２の起動前に既に接続されている場合には起動時）で、ＰＣ１０３へ使用可能のアクセスキー１０１を認識した事がアクセスキー１０１に記憶された認証用データ２０１と共に報告される。また、ＩＣカードリーダライタ１０２に使用可能／不可判別用データ２０２が使用不可を表しているアクセスキー１０１が接続されると、その時点（ＩＣカードリーダライタ１０２の起動前に既に接続されている場合には起動時）で、ＰＣ１０３へ使用不可のアクセスキー１０１を認識した事がアクセスキー１０１に記憶された認証用データ２０１と共に報告される。

【００２５】また、さらに、ＩＣカードリーダライタ１０２に接続されたアクセスキー１０１の使用可能／不可判別用データ２０２が書き換えられると、使用可能を表すデータに書き換えられた場合にはＰＣ１０３へ使用可能のアクセスキー１０１を認識した事がアクセスキー１０１に記憶された認証用データ２０１と共に報告され、使用不可を表すデータに書き換えられた場合にはＰＣ１０３へ使用不可のアクセスキー１０１を認識した事がアクセスキー１０１に記憶された認証用データ２０１と共に報告される。

【００２６】さて、ステップ４１１では、ＰＣ１０３から使用可能／不可判別用データ２０２の書き換え命令を受けたかどうかを調べ、受けている場合には、書き換え命令に従ってアクセスキー１０１の使用可能／不可判別用データ２０２を書き換え（ステップ４１２）、ステップ４１３に進む。一方、書き換え命令を受けていない場合には、そのままステップ４１３に進む。

【００２７】一方、先のステップ４０３においてアクセスキー１０１の認証用データ２０１と使用可能／不可判別用データ２０２を読み出すことができなかった場合には、ステップ４０４において、これまでアクセスキー１０１を認識していたかどうかを調べる。ここでは、具体

的には、前回行ったステップ４０２でアクセスキー１０１の認証用データ２０１と使用可能／不可判別用データ２０２を読み出すことができている場合には、これまでアクセスキー１０１を認識していたと判定し、他の場合は、これまでアクセスキー１０１を認識していなかったと判定する。ただし、今回行ったステップ４０２が起動後最初に行われたステップ４０２である場合には、これまでアクセスキー１０１を認識していなかったと判定する。そして、これまでアクセスキー１０１を認識していなかったと判定された場合には、ステップ４１３に移行し、これまでアクセスキー１０１を認識していたと判定された場合には、ＰＣ１０３にアクセスキー１０１が認識できなくなったことを報告し（ステップ４０５）、ステップ４１３に進む。結果、ＩＣカードリーダライタ１０２からアクセスキー１０１が取り外されると、ＰＣ１０３にアクセスキー１０１が認識できなくなったことが報告される。

【００２８】最後に、ステップ４１３では、ＰＣ１０３から終了命令を受けたかどうかを調べ、受けている場合には、ステップ４０１に、受けていない場合にはステップ４０２に戻る。

【００２９】次に、ＰＣ１０３のアクセスキー処理プログラム２０５の動作について説明する。

【００３０】図５に、アクセスキー処理プログラム２０５の動作手順を示す。

【００３１】図示するようにＰＣ１０３が起動されると、アクセスキー処理プログラム２０５が起動される。起動されたアクセスキー処理プログラム２０５は、ＩＣカードリーダライタ１０２にアクセスキー１０１の認識監視の開始命令を送信する（ステップ５００）。そして、最後にＩＣカードリーダライタ１０２から受け取った報告が使用可能もしくは使用不可のアクセスキー１０１を認識したことの報告となるまで待つ（ステップ５０１）。なお、ここで、まだ何の報告も受け取っていない場合には、これら報告を受信することにより最後にＩＣカードリーダライタ１０２から受け取った報告が使用可能もしくは使用不可のアクセスキー１０１を認識したことの報告となる。そして、最後にＩＣカードリーダライタ１０２から受け取った報告が使用可能もしくは使用不可のアクセスキー１０１を認識したことの報告となったならば、報告と共に受け取った認証用データ２０１を、あらかじめアクセスキー処理プログラム２０５に登録された認証データと比較することにより検証し（ステップ５０２）、正当なものでなければステップ５０１に戻り、正当なものであればステップ５０３に進む。

【００３２】ステップ５０３では、この最後に受け取った報告が使用可能のアクセスキー１０１を認識したことの報告であるかどうかを判定し（ステップ５０３）、そうであれば、ＯＳ２０６を起動、動作させる（ステップ５０７）。これにより、利用者はＰＣ１０３を利用可能となる。

【００３３】さて、ステップ５０７で、ＯＳ２０６を起動、動作させた後は、ユーザーからのキー入力、マウス入力などの各種入力を監視し、一定時間内に何らかの入力が利用者よりなされたかどうかを調べ（ステップ５０８）、一定時間内に入力がなかった場合は、ＩＣカードリーダライタ１０２に、アクセスキー１０１の使用可能／不可判別用データ２０２を使用不可を表すデータに書き換える使用可能／不可判別用データ２０２の書き換え命令を送信し（ステップ５０９）、ＯＳ２０６の動作を停止させ（ステップ５１１）、ステップ５０１に戻る。

【００３４】一方、一定時間内に入力があった場合は、同データを記憶したアクセスキー１０１を認識中かどうかを判定する（ステップ５１０）。ここでは、具体的には、先にステップ５０１の判定で最後の報告として取り扱った報告以降、何の報告もＩＣカードリーダライタ１０２から受け取っていない場合には、同データを記憶したアクセスキー１０１を認識中であると判定し、他の場合には、同データを記憶したアクセスキー１０１を認識中でないと判定する。そして、同データを記憶したアクセスキー１０１を認識中でないと判定された場合には、ＯＳ２０６の動作を停止させ（ステップ５１１）、ステップ５０２に戻る。

【００３５】一方、同データを記憶したアクセスキー１０１を認識中である場合には、利用者よりＯＳ２０６の終了を指示されているかどうかを調べ、指示されていない場合には、ステップ５０８に戻り、指示されている場合には、ＯＳ２０６を終了させ、ＩＣカードリーダライタ１０２に終了命令を発行し、処理を終了する。

【００３６】一方、先のステップ５０３において、最後の報告が使用不可のアクセスキー１０１を認識したことの報告であると判定された場合には、利用者に認証用データを入力させ（ステップ５０４）、入力された認証用データが正当なものであるかどうかを当該入力されたデータをあらかじめアクセスキー処理プログラム２０５に登録された認証データと比較することにより調べ（ステップ５０５）、入力された認証用データが正当なものであれば、ＩＣカードリーダライタ１０２に、アクセスキー１０１の使用可能／不可判別用データ２０２を使用可能を表すデータに書き換える使用可能／不可判別用データ２０２の書き換え命令を送信し（ステップ５０６）、ステップ５０７に進んでＯＳ２０６を起動、動作させる。一方、入力された認証用データが正当なものでなければステップ５０１に戻る。

【００３７】以上のような本実施形態に係る電子計算機システムの動作によれば、正当なアクセスキー１０１がＩＣカードリーダライタ１０２に接続されると、ＯＳ２０６を動作させ、利用者がアクセス可能とするが、その後、一定時間以上、利用者よりの入力が無かった場合には、アクセスキー１０１の正当な所持者がアクセスキー

１０１を放置したものと見なして、ＯＳ２０６を停止させ、かつ、アクセスキー１０１の使用可能／不可判別用データ２０２を使用不可を表すデータに書き換えＯＳ２０６を動作させることができないようにすることにより、他者の不正なアクセスを排除することができる。

【００３８】一方、このように使用不可にしたアクセスキー１０１が正当な所持者の手によって使用される場合には、再度、このアクセスキー１０１によってＯＳ２０６を動作させアクセスすることが可能となるように、正当な所持者の認証用データの入力によってアクセスキー１０１の使用可能／不可判別用データ２０２を使用可能を表すデータに書き換える。したがって、正当な所持者がアクセスキー１０１を放置せず、熟慮や居眠りなどにより、一定時間以上入力しなかったために、ＯＳ２０６が停止し、アクセスキー１０１が使用できなくなった場合にも、正当な利用者であれば、即座に、ＯＳを再動作させ、アクセスキーを使用可能とすることができる。

【００３９】以上、本発明の実施形態について説明した。

【００４０】なお、以上の実施形態において、ＩＣカードリーダライタ１０２において、ＰＣ１０３の電源を監視し、ＰＣ１０３の電源ＯＦＦ後、一定時間以上、アクセスキー１０１を認識し続けた場合には、アクセスキー１０１の使用可能／不可判別用データ２０２を使用不可を表すデータに書き換えるようにしてもよい。

【００４１】また、以上の実施形態では、アクセスキー１０１によりアクセスを可能とする対象を全アプリケーションプログラム２０７を含むＯＳ２０６上で実現される全機能としたが、これは、個々のアプリケーションプログラム２０７とするようにしてもよい。

【００４２】また、本実施形態に係るアクセスキーの技術は、電子計算機システムに限らず、任意の装置、システムに適用可能である。

【００４３】また、アクセスキーとしては、ＩＣカードの他、メモリカードや、その他の各種記録媒体を用いるようにしてもよい。

【００４４】また、以上の実施形態におけるＩＣカードリーダライタを、単に、アクセスキーの読み書きを行う装置とし、ＩＣカードリーダライタを介して、ＰＣ１０３が、先に図４に示した処理を行うようにしてもよい。

【００４５】また、図５のステップ５０５では、入力された認証データとアクセスキー１０１に記憶されている認証データを比較するようにしてもよい。

【００４６】また、以上の実施形態では、各アクセスキーの使用可能／不可を表す使用可能／不可判別用データを、個々のアクセスキーに記憶して使用したが、全てのアクセスキーについての使用可能／不可判別用データをＰＣ１０３側に記憶し、使用するようにしてもよい。ただし、この場合において、アクセスキーが複数のＰＣ１０３で使用されるものである場合には、ＰＣ１０３間で全てのアクセスキーについての使用可能／不可判別用データを交換し、各アクセスキーの使用可能／不可判別用データを最新の状態に維持するようにする。

【００４７】

【発明の効果】以上のように、本発明によれば、システム利用途中でアクセスキーをシステムに接続したまま、利用者がシステムを離れてしまった場合に、第三者による、システムへの不正なアクセスを排除することができる。

【図面の簡単な説明】

【図１】本発明の実施形態に係る電子計算機システムの構成を示すブロック図である。

【図２】本発明の実施形態に係る電子計算機システムのソフトウエア構成を示すブロック図である。

【図３】本発明の実施形態に係る電子計算機のハードウエア構成を示すブロック図である。

【図４】本発明の実施形態に係る認識監視処理プログラムの動作の手順を示すフローチャートである。

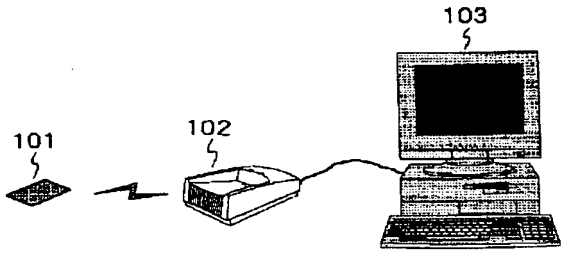
【図５】本発明の実施形態に係るアクセスキー処理プログラムの動作の手順を示すフローチャートである。

【符号の説明】

１０１　アクセスキー
１０２　ＩＣカードリーダライタ
１０３　ＰＣ
２０３　認識監視処理プログラム
２０５　アクセスキー処理プログラム

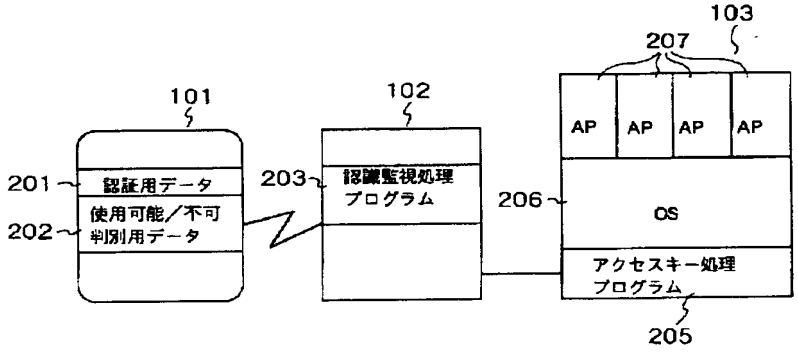
【図１】

図1



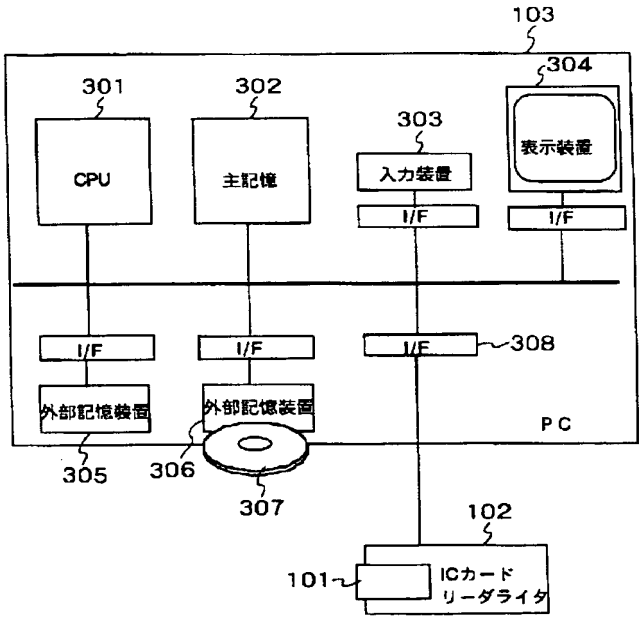
【図２】

図2



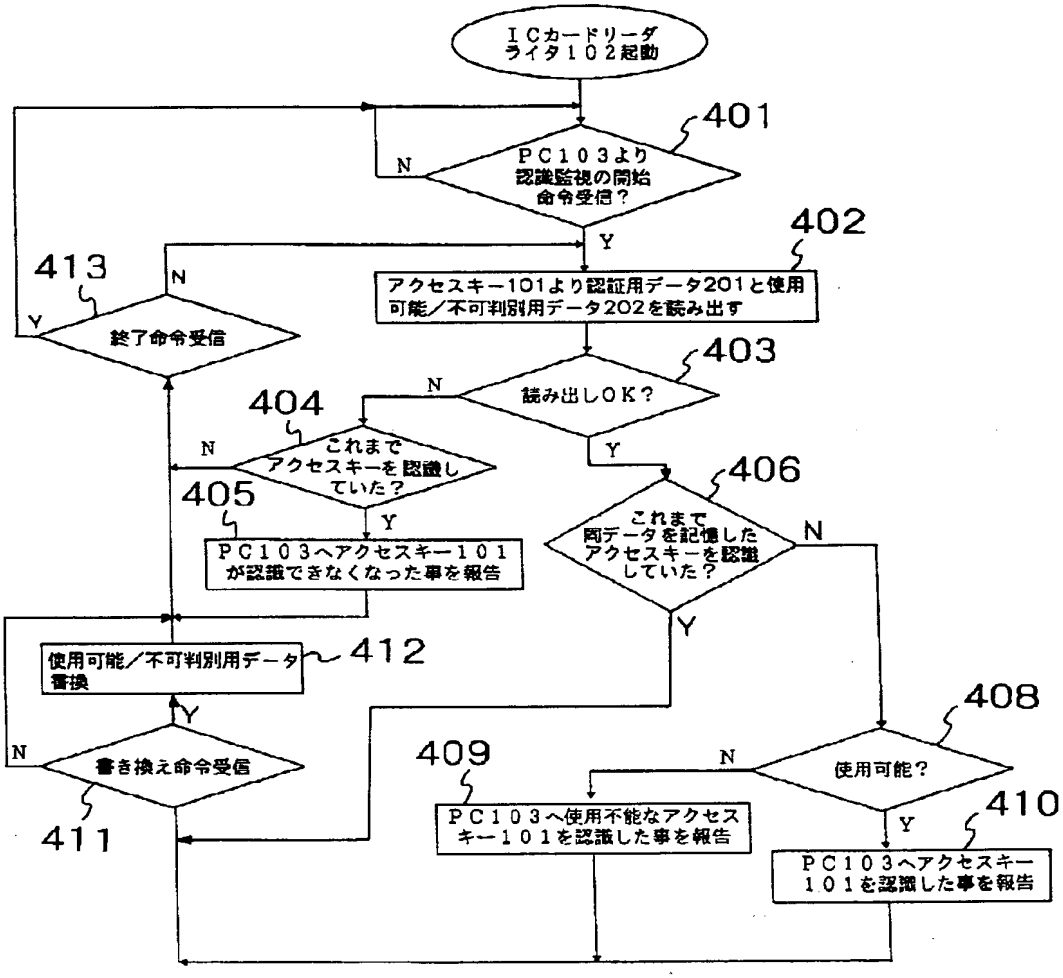
【図３】

図3



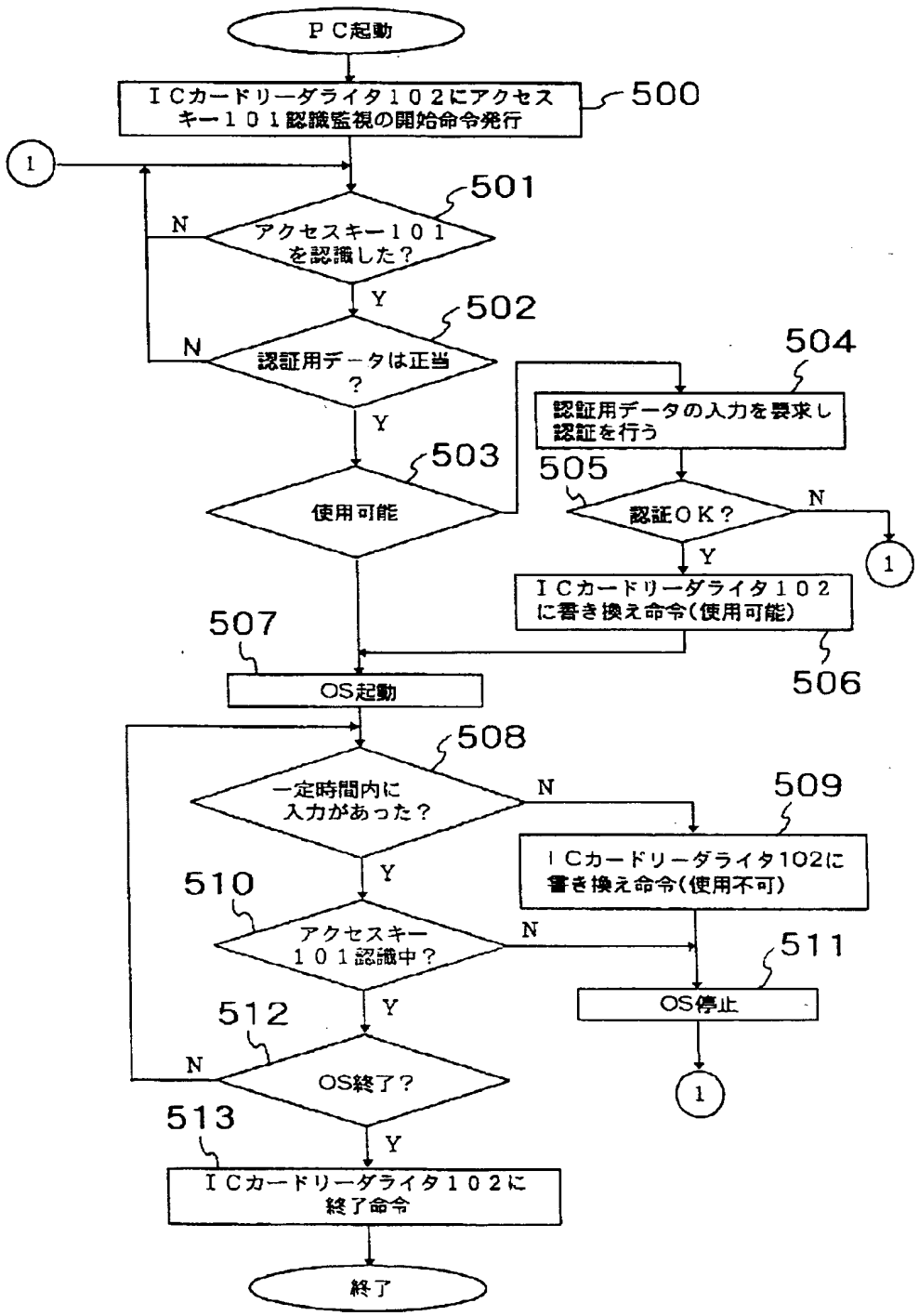
【図４】

図4


ＩＣカードリーダライタ１０２起動
401
ＰＣ１０３より認識監視の開始命令受信？
N
Y
402
アクセスキー101より認証用データ201と使用可能／不可判別用データ202を読み出す
403
読み出しＯＫ？
N
Y
404
これまでアクセスキーを認識していた？
N
Y
405
ＰＣ１０３へアクセスキー１０１が認識できなくなった事を報告
406
これまで同データを記憶したアクセスキーを認識していた？
N
Y
408
使用可能？
N
Y
409
ＰＣ１０３へ使用不能なアクセスキー１０１を認識した事を報告
410
ＰＣ１０３へアクセスキー１０１を認識した事を報告
412
使用可能／不可判別用データ書換
413
終了命令受信
N
Y
411
書き換え命令受信
N
Y

【図５】

図5


ＰＣ起動
ＩＣカードリーダライタ１０２にアクセスキー１０１認識監視の開始命令発行
500
1
501
アクセスキー１０１を認識した？
N
Y
502
認証用データは正当？
N
Y
503
使用可能
504
認証用データの入力を要求し認証を行う
505
認証ＯＫ？
N
Y
1
ＩＣカードリーダライタ１０２に書き換え命令（使用可能）
506
507
OS起動
508
一定時間内に入力があった？
N
Y
509
ＩＣカードリーダライタ102に書き換え命令（使用不可）
510
アクセスキー１０１認識中？
N
Y
511
OS停止
1
512
OS終了？
N
Y
513
ＩＣカードリーダライタ１０２に終了命令
終了